网页防篡改（原生版）

用户使用指南

天翼云科技有限公司

修订记录

内容	时间
新建	2021/11/12
修订	2021/12/14

目 录

1. 产品概述

1.1. 产品定义

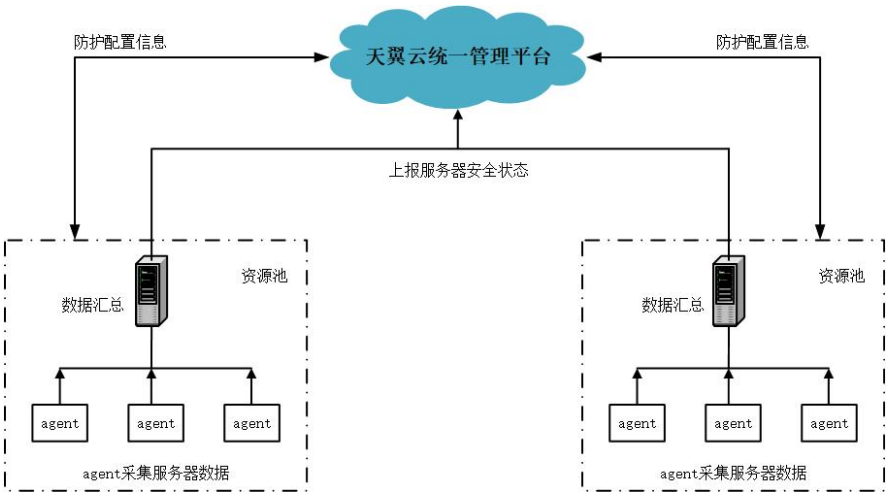
天翼云网页防篡改（原生版）产品（CT-WT，WebpageTampering）是一款全方位保障云上网站安全的产品，可对网站文件进行监控，若发生篡改时，实时对客户进行告警；同时通过备份恢复被篡改的文件或目录，保障客户系统的网站信息不被恶意篡改。

1.2. 产品功能

天翼云网页防篡改（原生版）产品通过 Agent 进行自动化采集，获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常变动进行告警和恢复。网页防篡改（原生版）产品主要包括以下 4 个功能：

- 篡改监测：针对云主机或物理机防护目录下的异常文件变动进行实时监测；
- 篡改告警：一旦发生异常的文件添加、修改和删除，立即进行客户告警；
- 文件备份：对云主机或物理机防护目录下的目录和文件，系统进行备份；
- 自动恢复：当防护文件发生异常的增删改问题时，通过备份进行实时恢复，保障客户系统的网站信息不被恶意篡改。

1.3. 产品架构



网页防篡改（原生版）产品是服务器安全卫士（基础版）的增值产品，使用相同的技术架构。

服务器安全卫士（基础版）整体架构主要包括 3 个部分，分别为天翼云统一管理平台、资源池数据汇总节点和服务器客户端 Agent。

- 天翼云统一管理平台：客户通过统一的天翼云统一管理平台，查看所有的服务器信息和安全状态，并下发安全策略配置信息。
- 资源池数据汇总节点：服务器客户端 Agent 从被监控服务器中采集系统信息，上报给相应的资源池数据汇总节点。
- 服务器客户端 Agent：使用天翼云服务器安全卫士（基础版）产品时，每台服务器客户端需安装一个 Agent。

1.4. 产品优势

- 方便易用

只需在 Web 服务器一键安装 Agent，简单配置防护策略即可实现防护，全部操作都有可视化界面，方便用户使用。

- 灵活配置

防护策略支持自定义配置，按需指定防护的进程和文件类型，支持各类网站文件的保护。

- 安全可靠

产品实现自我保护机制，防止被篡改，采用加密传输与服务端通信，保证数据安全。通过 5000+台服务器的运行实践，稳定性高达 99.998%，2 分钟内离线自动重启机制，保障系统始终处于检测状态。

- 节约资源

正常的系统负载情况下，CPU 占用率 <1%，内存占用 <40M，消耗极低 。在系统负载过高时，Agent 会主动降级运行（CPU 占用率 <1%），严格限制对系统资源的占用，确保业务系统正常运行。

1.5. 术语说明

- Agent：是服务器安全卫士（基础版）部署到用户云服务器操作系统中的轻量化进程，主要功能是根据用户配置的安全策略，上报服务器存在的安全风险和新增的安全事件数据，同时响应用户和安全卫士云端防护中心的指令，实现对云服务器上的安全威胁清除和恶意攻击拦截。
- 白名单模式：是一种防护配置模式。在白名单模式下，会对添加的防护目录和文件类型进行保护。
- 黑名单模式：是一种防护配置模式。在黑名单模式下，会防护目录下所有未排除的子目录、文件类型和指定文件。

1.6. 应用场景

天翼云网页防篡改（原生版）产品（CT-WT，WebpageTampering）具有广泛的应用场景，以下是三种常见的应用场景。

- 场景一：网站实时监管

政府、金融、交通等行业需要对网站进行实时监测，防止网站被植入涉恐、涉政、暗链、后门等，否则一旦网站出现被篡改问题，会严重影响政府、交通等单位形象，造成企业巨大损失。

- 场景二：重大活动保障

在重大活动保障期间，各行业的官网、业务系统等网站出现非法关键词，导致被监管单位通报，其声誉将受到影响，评分会受到严重影响。

- 场景三：等保合规

信息安全等级保护是我国信息安全保障的一项基本制度，要求网络经营者应符合网络安全等级保护制度的要求。天翼云网页防篡改（原生版）帮助有等保需求的用户，进行安全测评，满足等保合规的要求。

1.7. 与其他云服务关系

网页防篡改（原生版）产品是服务器安全卫士（基础版）的增值产品，使用相同的技术架构。

2. 购买指南

2.1. 计费说明

本文为您介绍天翼云网页防篡改（原生版）产品（CT-WT，WebpageTampering）的费用组成和计费模式。

标准资费

网页防篡改（原生版）产品提供包年包月计费方式。

网页防篡改（原生版）产品的具体价格如下：

计费项	计费单位	标准资费
网页防篡改（原生版）	元/个/月	980

针对一次性包年付费服务，网页防篡改（原生版）的优惠政策为：1 年 85 折、2 年 7 折、3 年 5 折。

2.2. 购买方式

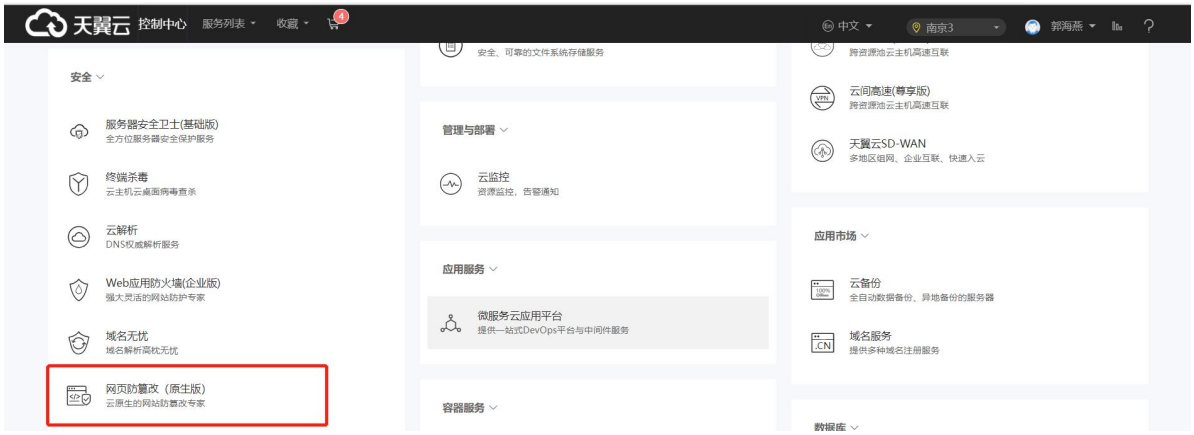
以下为网页防篡改（原生版）的购买流程。

当您具备已通过实名认证的 ctyun 账号后，可以通过以下三种方式开通网页防篡改（原生版）：

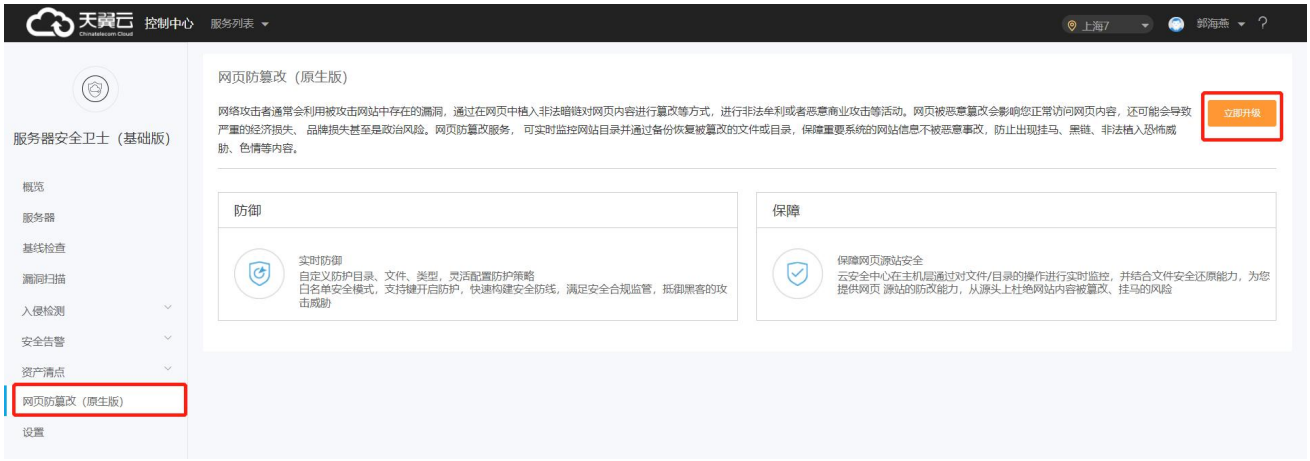
1. 进入网页防篡改（原生版）产品详情页，在产品版本中选择“网页防篡改（原生版）产品”，如下图所示：

单击【立即开通】，进入到网页防篡改（原生版）产品购买页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

2. 在天翼云控制台中，安全分类下，点击“网页防篡改（原生版）”，



进入网页防篡改（原生版）控制台，如下图所示：



点击“立即升级”，进入订购页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

3. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（基础版）”，进入服务器安全卫士（基础版）控制台，如下图所示：

在页面上单击“网页防篡改（原生版）”，进入网页防篡改（原生版）界面，如下图所示：

点击“立即升级”，进入订购页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

3. 快速入门

3.1. 注册天翼云账号

在创建和使用网页防篡改（原生版）之前，您需要先注册天翼云门户的账号。本节将介绍如何进行账号注册，如果您拥有天翼云的账号，请跳转到“开通网页防篡改（原生版）”。

1. 登录天翼云门户 http://www.ctyun.cn，点击【注册】；

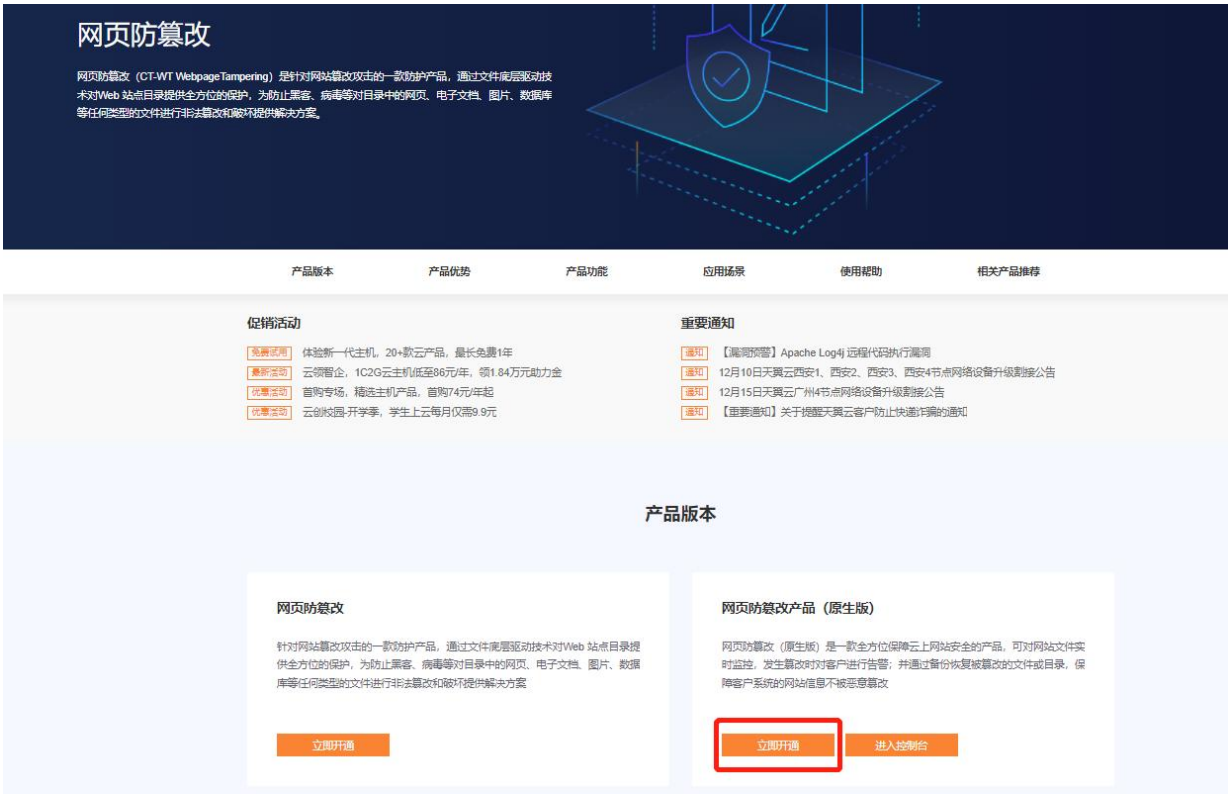
2. 在注册页面，请填写“邮箱地址”、“登录密码”、“手机号码”，并点击“同意协议并提交”按钮，如 1 分钟内手机未收到验证码，请再次点击“免费获取短信验证码”按钮；

3. 注册成功后，可到邮箱激活您的账号或立即体验天翼云。

3.2. 开通网页防篡改（原生版）

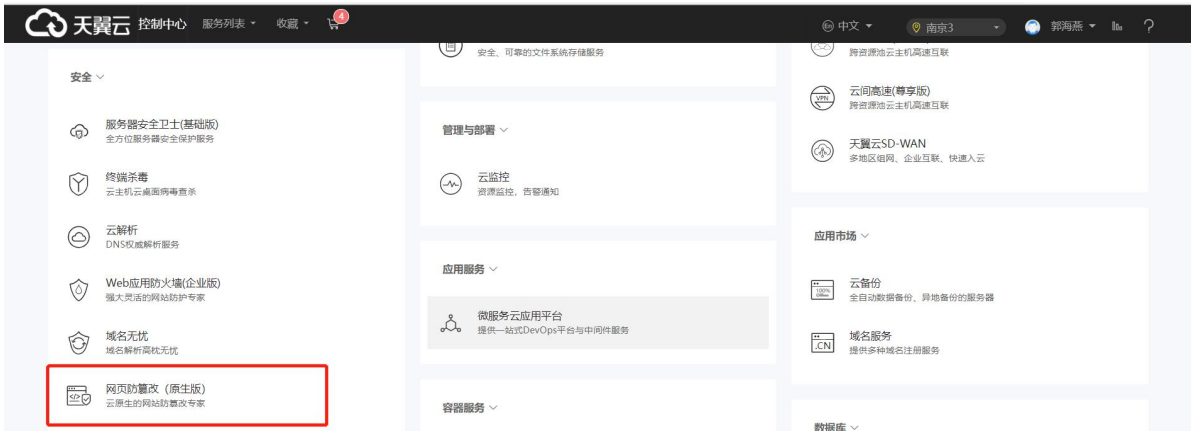
当您具备已通过实名认证的 ctyun 账号后，可以通过以下三种方式开通网页防篡改（原生版）：

1. 进入网页防篡改（原生版）产品详情页，在产品版本中选择“网页防篡改（原生版）产品”，如下图所示：

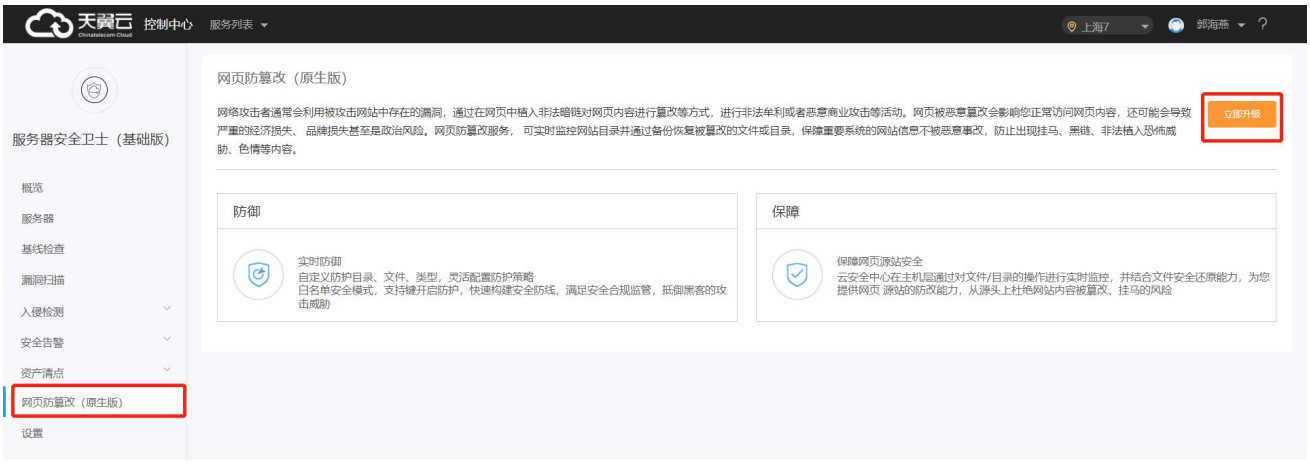


单击【立即开通】，进入到网页防篡改（原生版）产品购买页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

2. 在天翼云控制台中，安全分类下，点击“网页防篡改（原生版）”，



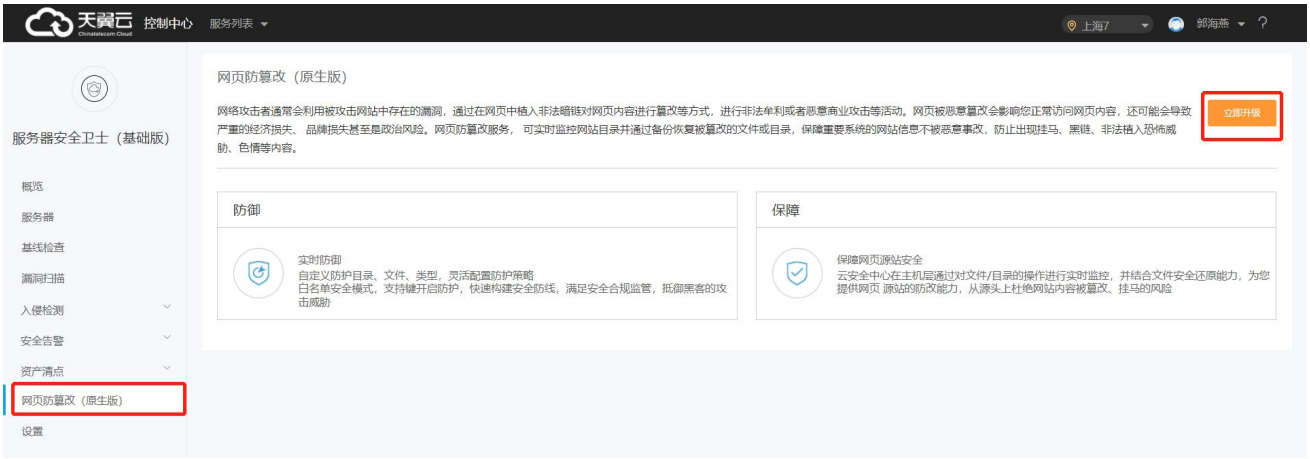
进入网页防篡改（原生版）控制台，如下图所示：



点击“立即升级”，进入订购页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

3. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（基础版）”，进入服务器安全卫士（基础版）控制台，如下图所示：

在页面上单击“网页防篡改（原生版）”，进入网页防篡改（原生版）界面，如下图所示：



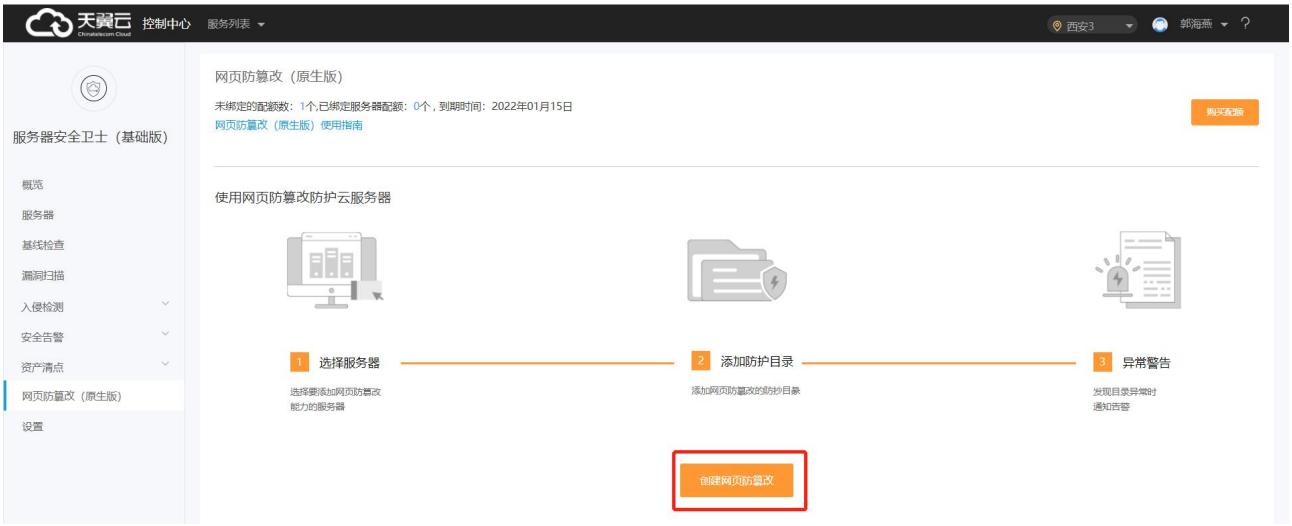
点击“立即升级”，进入订购页面，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可开通网页防篡改（原生版）服务，如下图所示：

3.3. 创建网页防篡改（原生版）

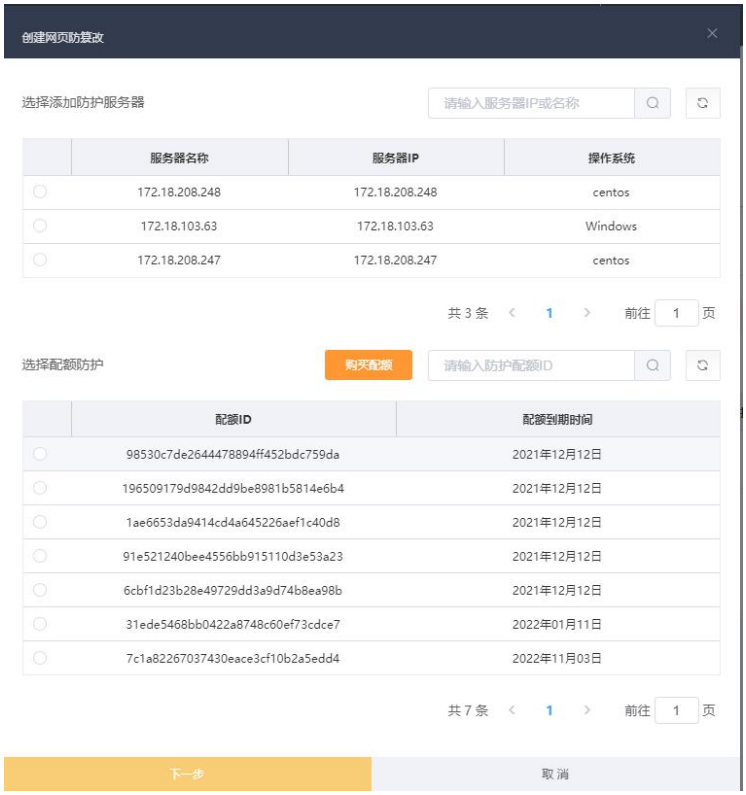
开通网页防篡改（原生版）后，可通过控制台创建网页防篡改（原生版）的监测防护。

操作步骤：

1. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（基础版）”或“网页防篡改（原生版）”；
2. 在已购买的资源池下，进入“创建网页防篡改（原生版）”页面；



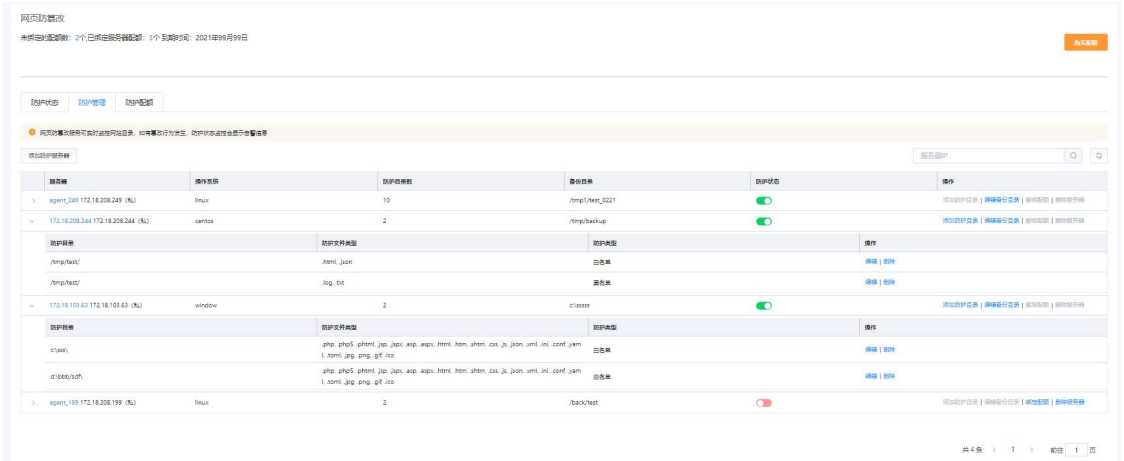
3. 单击**“创建网页防篡改”**，在弹出的创建网页防篡改（原生版）对话框中，根据页面提示进行配置，配置顺序为：添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护；



4. 该服务器列表中，展示用户当前资源池所有的防护列表的云主机/物理机；配额列表中，展示用户当前资源池所有的配额。选择需要防护的服务器，并选择配额后，方可进入下一步；

5. 添加防护目录分为添加白名单或添加黑名单 2 种模式，上图为白名单模式。选择防护目录、防护文件类型和本地备份目录，点击“开启防护”后，即开始对配置的文件进行防护；

6. 上图为黑名单模式。选择防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，点击“开启防护”后，即开始防护目录下所有未排除的子目录、文件类型和指定文件；



7. 开启防护后，进入防护服务器列表，展示该资源池中的已添加防护的服务器，以及每台服务器已配置的防护目录情况。

4. 操作指南

4.1. 网页防篡改（原生版）概述

天翼云网页防篡改（原生版）产品通过 Agent 进行自动化采集，获取被保护的服务器中写防护目录下文件的进程列表，实时识别异常进程和异常文件变动，并对异常变动进行告警和恢复。

支持的系统

支持 64 位的 linux 和 windows 系统下文件的防篡改，详情见下表：

OS	支持的 OS 版本
Windows（64 位）	● Windows 2008 ● Windows 2012 ● Windows 2016
CentOS（64 位）	● CentOS 6 ● CentOS 7 ● CentOS 8
Ubuntu（64 位）	● Ubuntu 16 ● Ubuntu 18

防护状态

可查看防护的总体情况，帮助您实时的掌握所有云上网站被篡改的总体态势。

功能	说明
防护总览	● 查看今日文件变动数 ● 查看最近 15 天文件变动数 ● 查看防护服务器数 ● 查看防护目录数 ● 查看防护文件总数 ● 查看未绑定/已绑定服务器配额数
防护文件状态图	● 查看防护文件类型分布（最近 15 天）统计图 ● 查看文件变动数 Top5（最近 15 天）统计图

功能	说明
告警列表	● 展示文件增加、删除、修改异常的告警列表
告警查询	● 根据时间、服务器 IP 和告警名称进行告警筛选和查询
告警忽略	● 若当前告警不需要再展示，选择忽略或批量忽略操作后，则该告警不再展示在列表中

防护管理

可为您账号下的云主机和物理机添加防护目录，可采用白名单或黑名单的方式进行添加。可展示当前已添加的服务器的防护目录和备份目录，并进行添加、编辑和删除。

功能	说明
创建网页防篡改（原生版）	● 适用于首次订购后创建网页防篡改（原生版）
添加防护服务器	● 适用于非首次订购，对需防护的服务器添加防护策略
防护服务器列表	● 显示防篡改实例服务器列表 ● 变更防护状态：开启/关闭 ● 添加防护目录 ● 编辑备份目录 ● 解绑配额 ● 绑定配额 ● 删除服务器
防护目录管理	● 显示服务器防护目录列表 ● 编辑防护目录设置 ● 删除防护目录

防护配额

展示订购配额的总体情况，同时可进行配额订购、续订和退订。

功能	说明
配额使用统计	● 正常配额的使用统计

功能	说明
配额状态统计	● 所有配额的状态统计
配额列表	● 展示配额情况的列表，包括配额 ID、配额状态、绑定服务器、使用状态、配额到期时间和操作
配额计费	● 配额订购 ● 配额续订 ● 配额退订 ● 到期处理

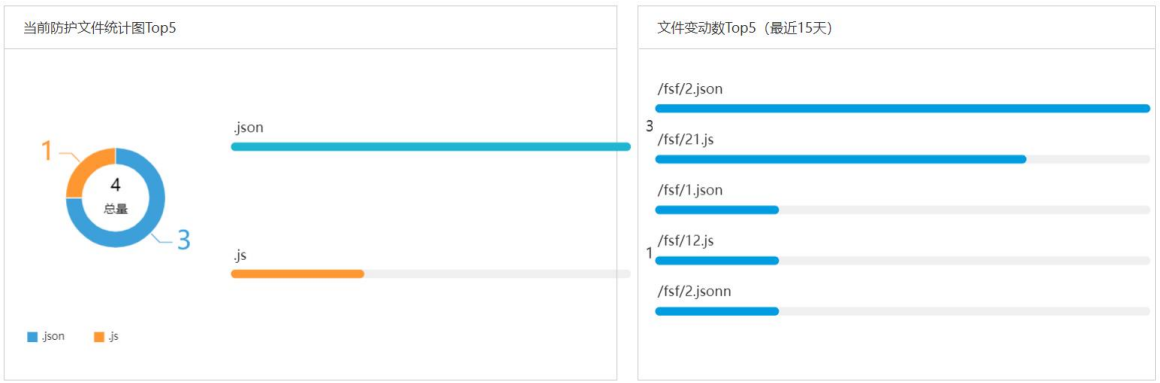
4.2. 防护状态

4.2.1 防护总览

如下图所示，您可查看该资源池的今日文件变动数、最近 15 天文件变动数、防护服务器数、防护目录数、防护文件总数、未绑定/已绑定服务器配额数。

4.2.2 防护文件状态图

如下图所示，您可查看当前防护文件统计图 Top5（最近 15 天）和文件变动数 Top5（最近 15 天）的统计图。



4.2.3 告警列表

如下图所示，您可查看文件增加、删除、修改异常的告警列表，包括告警等级、告警名称、受影响服务器、文件路径、时间、防护状态和操作。

4.2.4 告警查询

如下图所示，您可根据时间、服务器 IP 和告警名称进行告警筛选和查询，可选时间为最近一周、最近一月和最近三月。

4.2.5 告警忽略

如下图所示，若当前告警不需要再展示，选择忽略或批量忽略操作后，则该告警不再展示在列表中。

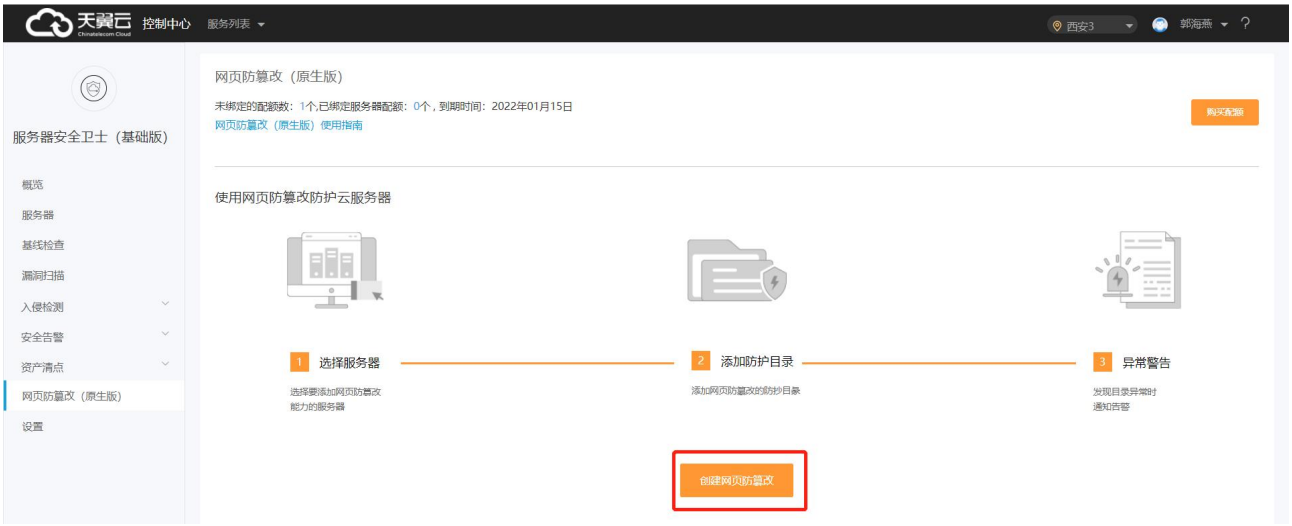
4.3. 防护管理

4.3.1 创建网页防篡改（原生版）

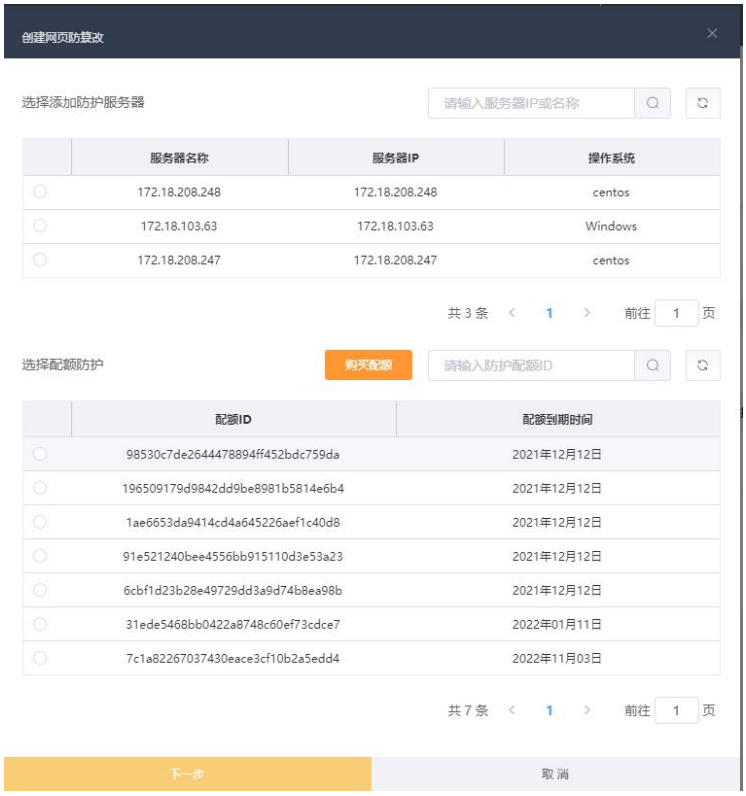
本节为您介绍在控制台创建网页防篡改（原生版）的操作步骤。

操作步骤：

1. 在天翼云控制台中，安全分类下，点击“服务器安全卫士（基础版）”或“网页防篡改（原生版）”；
2. 在已购买的资源池下，进入“创建网页防篡改”页面；



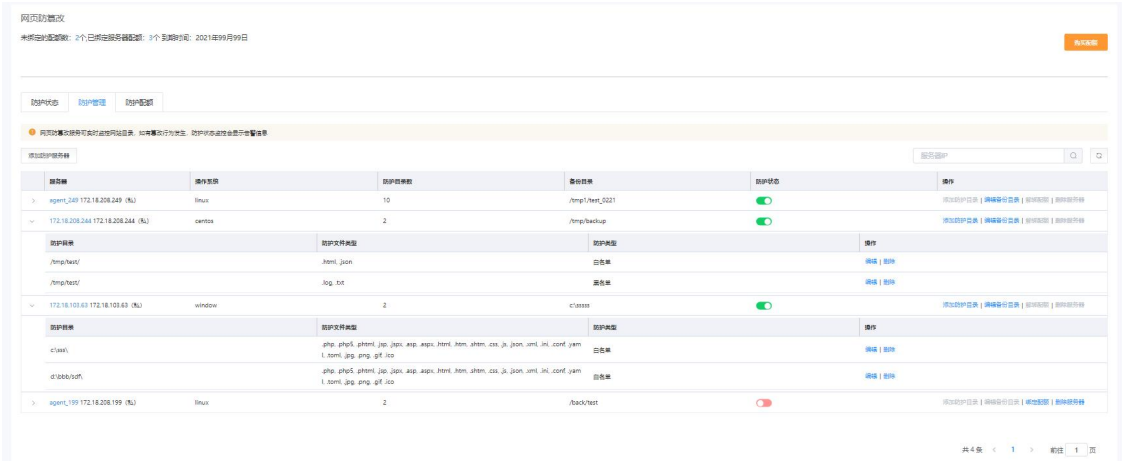
3. 单击**“创建网页防篡改”**，在弹出的创建网页防篡改对话框中，根据页面提示进行配置，配置顺序为：添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护；



4. 该服务器列表中，展示用户当前资源池所有的防护列表的云主机/物理机；配额列表中，展示用户当前资源池所有的配额。选择需要防护的服务器，并选择配额后，方可进入下一步；

5. 添加防护目录分为添加白名单或添加黑名单 2 种模式，上图为白名单模式。选择防护目录、防护文件类型和本地备份目录，点击“开启防护”后，即开始对配置的文件进行防护；

6. 上图为黑名单模式。选择防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，点击“开启防护”后，即开始防护目录下所有未排除的子目录、文件类型和指定文件；

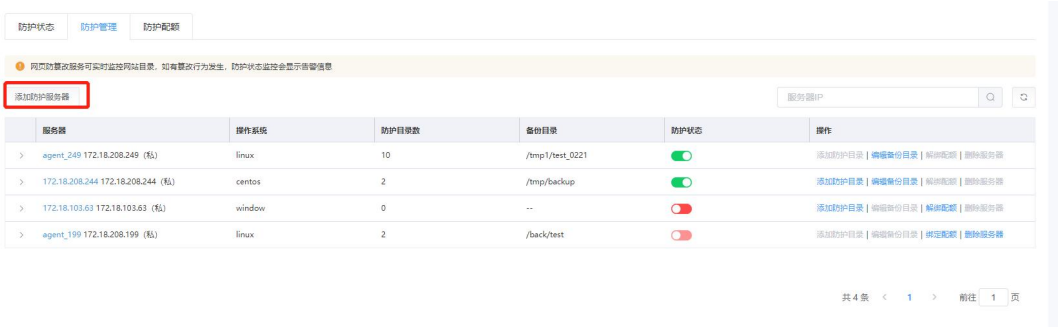


7. 开启防护后，进入防护服务器列表，展示该资源池中的已添加防护的服务器，以及每台服务器已配置的防护目录情况。

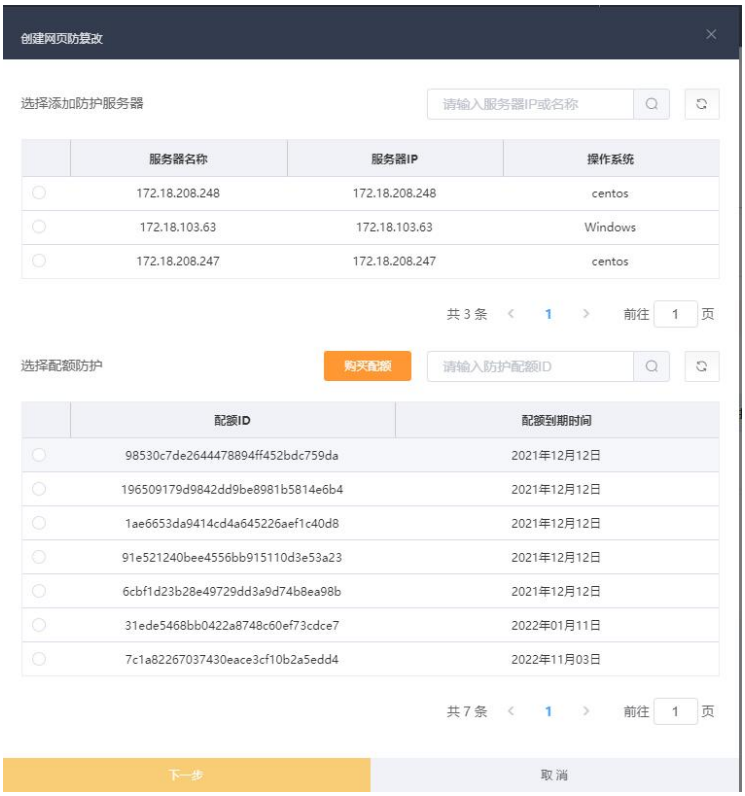
4.3.2 添加防护服务器

本节为您介绍添加防护服务器的操作步骤。

1. 点击防护管理页面的“添加防护服务器”，弹出“创建网页防篡改”对话框；



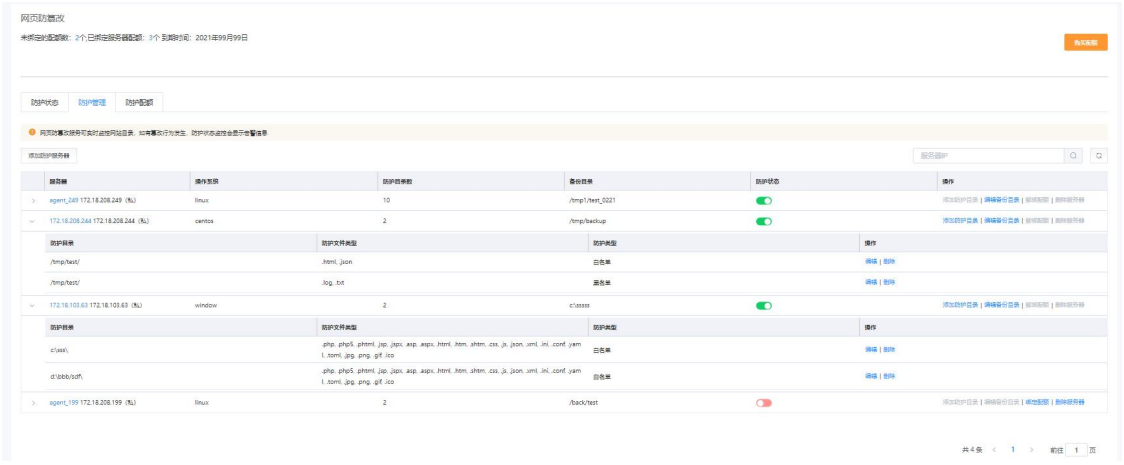
2. 在弹出的创建对话框中，根据页面提示进行配置，配置顺序为：添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护；



3. 该服务器列表中，展示用户当前资源池所有的防护列表的云主机/物理机；配额列表中，展示用户当前资源池所有的配额。选择需要防护的服务器，并选择配额后，方可进入下一步；

4. 添加防护目录分为添加白名单或添加黑名单 2 种模式，上图为白名单模式。选择防护目录、防护文件类型和本地备份目录，点击“开启防护”后，即开始对配置的文件进行防护；

5. 上图为黑名单模式。选择防护目录、排除子目录、排除文件类型、排除指定文件和本地备份目录，点击“开启防护”后，即开始防护目录下所有未排除的子目录、文件类型和指定文件；

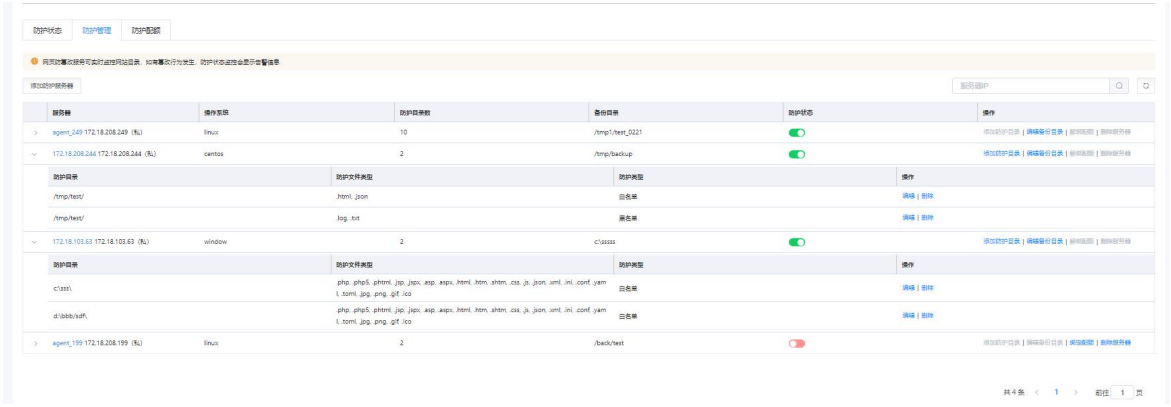


6. 开启防护后，进入防护服务器列表，展示该资源池中的已添加防护的服务器，以及每台服务器已配置的防护目录情况。

4.3.3 防护服务器列表

本节为您介绍已经添加的防护服务器列表。

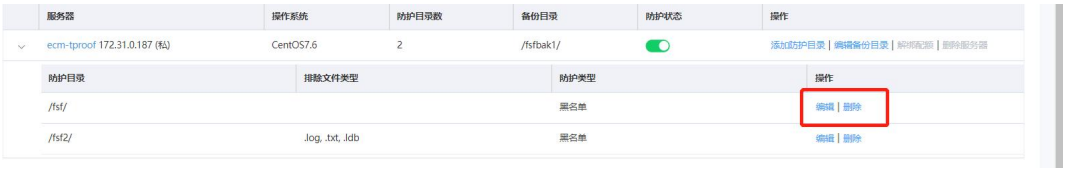
为您展示当前已添加的服务器的列表，包括添加服务器的名称、IP、操作系统、防护目录数和备份目录，可以对该服务器的防护状态进行开启/关闭，并可进行添加防护目录、编辑备份目录、绑定/解绑配额和删除服务器。



4.3.4 防护目录管理

本节为您介绍已添加防护服务器的防护目录管理。

可对服务器已添加的防护目录进行编辑、删除操作，如下图所示：



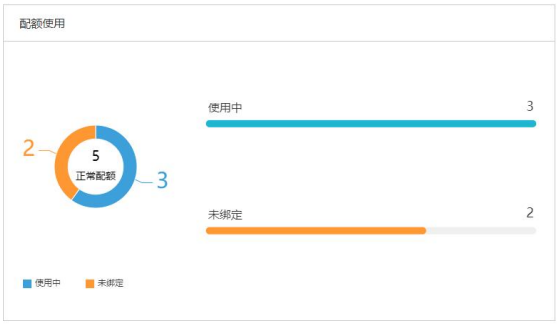
点击“编辑”时，弹出“编辑防护目录”对话框，可对您已经添加的防篡改策略进行修改。

点击“删除”时，弹出“删除”对话框，可对您已经添加的防篡改策略进行删除。

4.4. 防护配额

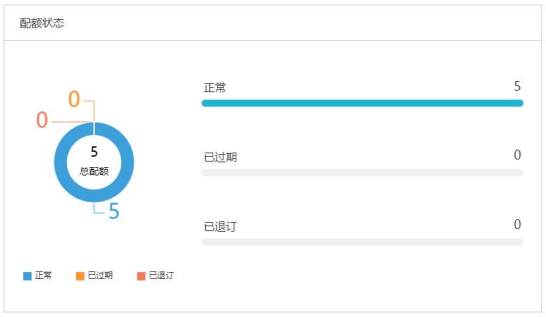
4.4.1 配额使用统计

为您展示正常配额的使用情况统计，分为使用中和未绑定 2 种状态。



4.4.2 配额状态统计

为您展示所有配额的使用情况统计，分为正常、已过期和已退订 3 种状态。



4.4.3 配额列表

配额列表展示正常、已到期、已退订 3 种状态的配额，销毁的配额不展示在列表中，分资源池进行展示，包括配额 ID、配额状态、绑定服务器、使用状态、开通时间、到期时间、操作等信息。

配额ID	配额状态	绑定服务器	使用状态	开通时间	到期时间	操作
9adf1627b9eb414584b67ddcf17fca02	正常		未绑定	2021年12月14日	2022年01月13日	续订 退订
7ecae55df8904df98b40461a847a7f3b	正常		未绑定	2021年12月14日	2022年02月12日	续订 退订
1ba3fa89c87749a5a702d8f787731a1c	正常		未绑定	2021年12月13日	2022年02月11日	续订 退订
1f3fd49e739f4e2098cbbcc9f71463c7	正常	ecm-tproof 172.31.0.187 (私)	使用中	2021年12月10日	2022年11月05日	续订 退订
5eca753c23424bfcbd29960f4bba7714	正常		未绑定	2021年12月10日	2022年11月05日	续订 退订
88ac82489bf1424db39fffab7fdb8e70	正常		未绑定	2021年12月09日	2024年12月08日	续订 退订
081e6efed383439fa26909e2c091d887	正常		未绑定	2021年12月09日	2025年05月28日	续订 退订
838dbc056edd46b6ac6ee2b1ec523548	正常		未绑定	2021年12月09日	2022年11月30日	续订 退订
55619156aebf4a1d8313db51dd0cfc53	正常		未绑定	2021年12月09日	2022年01月08日	续订 退订

4.4.4 配额计费

本节为您展示配额计费的相关操作，包括配额订购、配额续订、配额退订和到期处理相关操作。

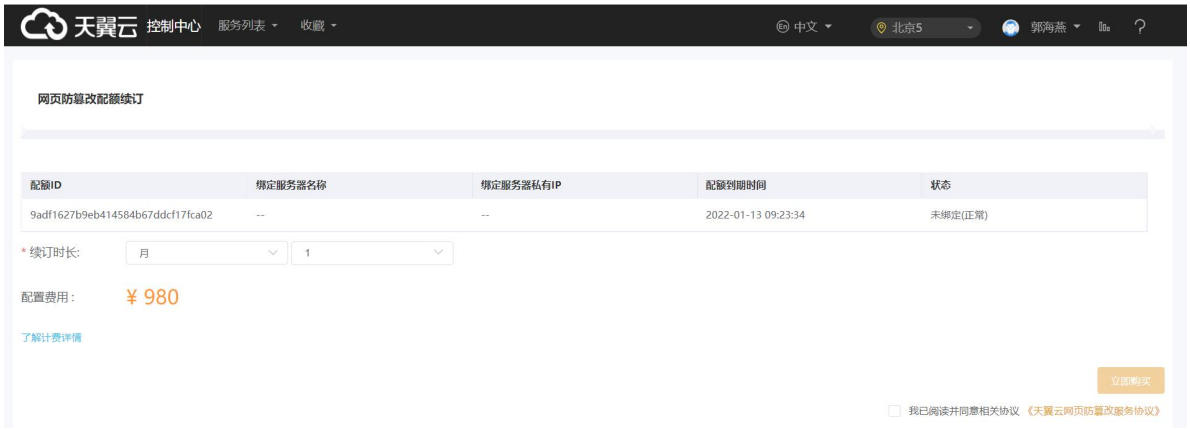
配额订购：前面已详述，此处不再赘述。

配额续订：客户可对已订购的网页防篡改（原生版）配额进行续费，需要此配额此时的状态为未到期、已到期。

如下图所示，对需要续订的配额，点击“续订”：

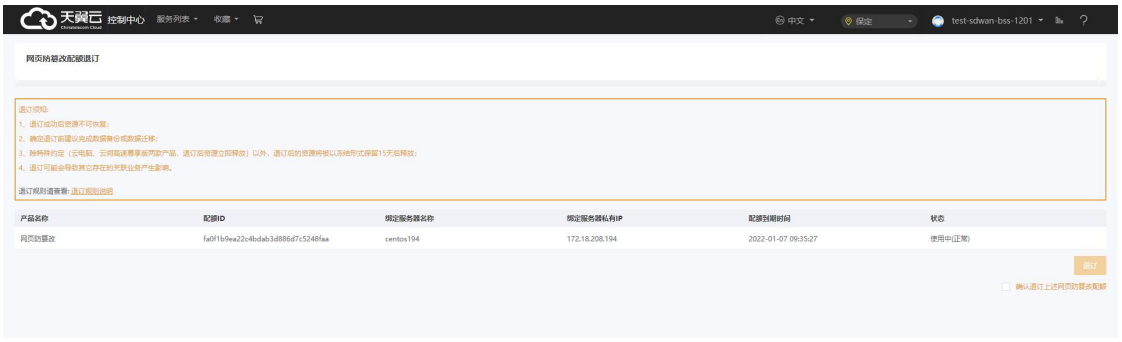
配额ID	配额状态	绑定服务器	使用状态	配额到期时间	操作
98530c7de2644478894ff452bdc759da	正常	(私)	未绑定	2021年12月12日	续订 退订
196509179d9842dd9be8981b5814e6b4	正常	(私)	未绑定	2021年12月12日	续订 退订
1ae6653da9414cd4a645226aef1c40d8	正常	(私)	未绑定	2021年12月12日	续订 退订
8ed1bef235154ecebdcff6bfdc9a5951	已过期	(私)	已过期	2021年11月12日	续订 退订
91e521240bee4556bb915110d3e53a23	正常	(私)	未绑定	2021年12月12日	续订 退订
6cbf1d23b28e49729dd3a9d74b8ea98b	正常	(私)	未绑定	2021年12月12日	续订 退订
31ede5468bb0422a8748c60ef73cdce7	正常	(私)	未绑定	2022年01月11日	续订 退订
7c1a82267037430eace3cf10b2a5edd4	正常	(私)	未绑定	2022年11月03日	续订 退订
7babdf892f5743a8a797d60d9654c4e4	正常	(私)	未绑定	2021年12月14日	续订 退订
de35c0825acd4978a0caeb4345b05be6	正常	(私)	未绑定	2021年12月14日	续订 退订

进入“续订”页面后，选择该配额需续订的时长，勾选我已阅读，理解并接受《天翼云网页防篡改（原生版）协议》，点击“立即购买”按钮，即可对该配额的网页防篡改（原生版）服务进行续费，如下图所示：



配额退订：根据您的需求，可对正常状态的配额进行退订，遵循天翼云统一的退订规则。如下图所示，对需要退订的配额，点击“退订”：

进入“退订”页面后，您需要进行确认退订的规则和金额，点击“退订”按钮，即可对该配额的网页防篡改（原生版）服务进行退订，如下图所示：



到期处理：您购买的全部配额均到期后，进入网页防篡改（原生版）页面后，会提醒您进行购买。

5. 常见问题

5.1. 计费类

Q：网页防篡改（原生版）的计费方式是什么？

A：网页防篡改（原生版）为包周期计费，分为按月和按年 2 种方式。

Q：网页防篡改（原生版）的计费项是什么？

A：网页防篡改（原生版）是服务器安全卫士（基础版）的增值产品，计费项是您订购的 Agent 配额个数，您选定配额个数和订购时长后，系统可自动计算出您的计费情况。

Q：网页防篡改（原生版）的配额续费条件是什么？

A：您所需续费的配额，需要为未到期或已到期状态。

5.2. 操作类

Q：如何使用网页防篡改（原生版）？

A：您首先需要根据所需防护的服务器上的网站情况，订购网页防篡改（原生版）配额，每台服务器需订购 1 个配额。订购成功后创建网页防篡改（原生版），根据您的网站情况进行防护策略的配置后，即可开启网页防篡改（原生版）防护服务。

Q：添加防护服务器的步骤是什么？

A：具体步骤为添加服务器->添加防护目录->添加防护文件类型->添加本地备份目录->开启防护，详情见添加防护服务器的操作步骤详情。

5.3. 系统类

Q:安装 agent 会不会对自身的业务稳定性产生影响？

A: 不会。agent 是纯应用层的，不会给系统装任何的驱动，不会影响系统的稳定性；agent 的带宽和资源占用很小；agent 已经通过各种业务场景长时间运行测试。

Q：用户配置的防护策略有什么限制？

A：Linux 系统单个防护目录大小不超过 2G。

Q：支持的系统 OS 有哪些？

A：支持 64 位的 linux 和 windows 系统下文件的防篡改，详情见下表：

OS	支持的 OS 版本
Windows（64 位）	● Windows 2008 ● Windows 2012 ● Windows 2016
CentOS（64 位）	● CentOS 6 ● CentOS 7 ● CentOS 8
Ubuntu（64 位）	● Ubuntu 16 ● Ubuntu 18